



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/357,483	07/20/1999	STEPHEN MICHAEL MATYAS JR.	5577-170	9314

20792 7590 05/23/2003

MYERS BIGEL SIBLEY & SAJOVEC  
PO BOX 37428  
RALEIGH, NC 27627

EXAMINER

KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 05/23/2003

5

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/357,483

Applicant(s)

MATYAS ET AL.

Examiner

Paula W Klimach

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 20 July 1999.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☐ Claim(s) 1-22 and 25 is/are rejected.
- 7) ☐ Claim(s) 23, 24, 26, 27 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

## Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5.
- 4) ☐ Interview Summary (PTO-413) Paper No(s) \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

## DETAILED ACTION

### *Specification*

The disclosure is objected to because of the following informalities:

On page 1 line 6 and 13, the attorney docket is supplied with the related cases.

The office asks that the attorney's docket number be removed..

Appropriate correction is required.

### *Claim Rejections - 35 USC § 101*

1. **Claim 1-22** are rejected under 35 U.S.C. 101 because it is not within technical art. Claim 1 discloses an algorithm.
2. As per claim 1, a review of the specification discloses that the claimed invention is directed to non-statutory software in the form of software alone with no tangible elements. For example claim 1 recites obtaining seed and randomized values, and dividing values into potential range of RSA encryption are found on pages 22-25 of the disclosure. Generating a first initial value based on the first seed value  $W_p$  and the second seed value  $W_q$  and the randomized values  $IV_p$  and  $IV_q$ , these generation steps for  $XX_p$  and  $XX_q$  are disclosed on page 22 lines 26-34 and page 23 lines 16-23 respectively. The mapping steps to provide  $X_p$  and  $X_q$  are disclosed on page 23 lines 0-15 and page 23 lines 23-32 respectively. The generation step and the mapping step are clearly mathematical computations with no tangible elements involved.
3. As per claim 22, the means for generating  $XX_p$  and  $XX_q$  and means for mapping to provide  $X_p$  and  $X_q$  are, as disclosed in the discussion of claim 1, mathematical computations with no tangible elements involved.

Art Unit: 2131

4. Dependent claims 2-21 add additional software elements or recite further details on the elements already recited in claim 1. Thus no statutory subject matter is added by these claims.

***Claim Rejections - 35 USC § 103***

5. **Claims 1, 2, 3, 11, 12, 22, and 25** are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest in view of Borza et al (6,215,874 B1).

In reference to claims 1, 22, and 25, Rivest discloses a system for finding RSA values, abstract. On page 9, Rivest discloses that p and q are large “random” primes used for RSA key generation. However Rivest does not discuss the method used to find the random numbers.

Borza discloses a method and system for generating random numbers, abstract, that uses biometrics, column 4 lines 28-31.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the biometric random number generator to find the two large random primes for RSA. One of ordinary skill in the art would have been motivated to do this because it would reduce the chances of predicting the random number, column 3 lines 25-29.

In reference to claim 2, Rivest discloses a method of finding the prime divisors p and q, page 9.

In reference to claim 3, 11 and 12, the prime divisors are generated using random numbers. Borza discloses the random number generation as being based on a biometric. The Borza random number generator based on a fingerprint whose image is taken by a biometric sensing device, column 4 lines 29-51.

6. **Claim 8** is rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest and Borza as applied to claim 1 above, and further in view of Soutar et al (6,219,794).

Art Unit: 2131

Rivest discloses a method of generating RSA cryptographic values, and Borza discloses a method of generating a random number using a biometric. However, neither Borza nor Rivest discloses a method for using a biometric by calculating a value using the biometric information to create a biometric template.

Soutar discloses a method for using a biometric by calculating a value using the biometric information to create a biometric template, Fig. 1.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Soutar method to calculate a biometric template. One of ordinary skill in the art would have been motivated to do this because the key cannot be released from the protected filter other than via the interaction with the correct biometric image, Soutar abstract.

#### ***Allowable Subject Matter***

Claims 23, 24, 26 and 27 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

#### ***Conclusion***

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Rivest	A Method for Obtaining Digital Signatures and Public-Key Cryptosystems
Borza et al	6, 215, 874 B1
Soutar et al	6, 219, 794 B1

Art Unit: 2131

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421.

The examiner can normally be reached on Mon to Fri 7:15 a.m to 3:45 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes can be reached on (703) 305-9711. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-8421 for regular communications and (703) 305-8421 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-4832.

PWK  
May 19, 2003



**GAIL HAYES**  
**SUPERVISORY PATENT EXAMINER**  
**TECHNOLOGY CENTER 2100**